Security Problems in VPN and Solutions

[1]Swapan Debbarma, [2]Agnivesh Pandey,
[1,2]Assistant Professor,
[1]Computer Science & Engineering Department,
[1]NIT Agartala, India,
[2]Department of information technology, School of studies in engineering and technology,
[2]Guru Ghasidas Vishwavidyalaya, Koni bilaspur, *Chhattisgarh, India*

Abstract: The importance of networks security and services at higher education institutions has never been higher than it is now. Users and institutions are demanding more and more network services and the exchange of more potentially sensitive information within these services. Firstly, in campus there is definite requirement of the network access. In order to enable learners to go beyond the limitations of space and time to acquire knowledge; in order to provide excellent learning environment for greater freedom and greater choice of learning activities space, the project to building campus network has become the basis of all university building work. It is related to the quality and level of their teaching and scientific research work. The campus network has a number of tasks such as teaching, research, management and communication with the outside. Therefore, the issue of network security has become a priority to campus network management. Obviously, the current Internet is convenient but at the same time it is unsafe. While using network services in campus network it can be more easily attacked. This paper represent the current security status of the campus network, analyze security threat to campus network and describe the strategies to maintenance of network security, so as to maintain an effective as well as robust network system. This paper will also introduce various current network information security problem and its solutions.

IndexTerms – VPN, Campus network, Network security, Security technology, Security threat, Firewalls

I. INTRODUCTION

Network is important for a society from very ancient age. A good network (fast, efficient and leakage proof) play vital role in establishment of any government, research organization, or business establishment. In the age of Information Technology, ancient information network converted into computer network which is very fast and easily manageable. Similar to ancient era computer network security threat is always a serious issue and is very crucial. A campus network is an autonomous network under the management of university campus or within a local geographic area such as a business park, a government institution, a research center, or a medical center. While the network may be managed by a single entity, it may be used by different organizations. The campus network has matured and grown more complex than ever. Often, a campus network provides and access path into a larger network, such as a metropolitan area network or the Internet. To build a stable, safe, efficient, convenient wireless campus network has become the inevitable trend of development and construction of campus network.

Computer network administrator faces many challenges in the process of maintaining high availability, good performance, and security. In a network there are several user groups which have different set of resource accessibility. Network operators may wish to allow only certain users access to various parts of the network; they may also aim to prevent certain sensitive data from "leaking" between different parts of the network, or from the internal network to the global Internet. It is difficult for network administrator to translate these types of high-level policy and design goals at level of individual devices, not based on a global perspective of the network.

There are two primary goals to design a data sharing system in campus network: First, from a user's perspective, users must have control on their data sharing system through which they can decide which web site they want to share and should also be aware of what happened to their data. Second, in campus network design, existing infrastructure must be utilized.

With the rapid expansion of the campus network connectivity, the network applications have increased rapidly, at the same time, the campus network information security has caused more attention today. Two areas where high-level problem is particularly acute are access control (defining who has access to what information and services on the network) and information flow control (defining where on the network, various information should be allowed to travel).

Almost no security measures has been taken in the existing network and application systems, and above this, security vulnerabilities in the host operating system and application system are also without any processing. There are many problems within system management; all of these formed a serious security problem, thus seriously threatening the safety of the campus network. In the recent network monitoring, system and the host was found to attempt to be invaded by others, a large number of security vulnerabilities exists in the system, and there are many security vulnerabilities which are difficult to avoid and eradicate. Also, a virus transmitted through the network severely affected the normally running of the campus network. Network traffic consumption attacks are another serious threat for network management. These attacks (e.g. Distributed Denial of Service attacks, Smurf Attack, TCPSYN Flood attack) are passive network attacks where network traffic is consumed up by unnecessary flow of data, preventing legitimate user to use network path. In this attack speed of network traffic is slow down to such a level that user cannot use network resources.

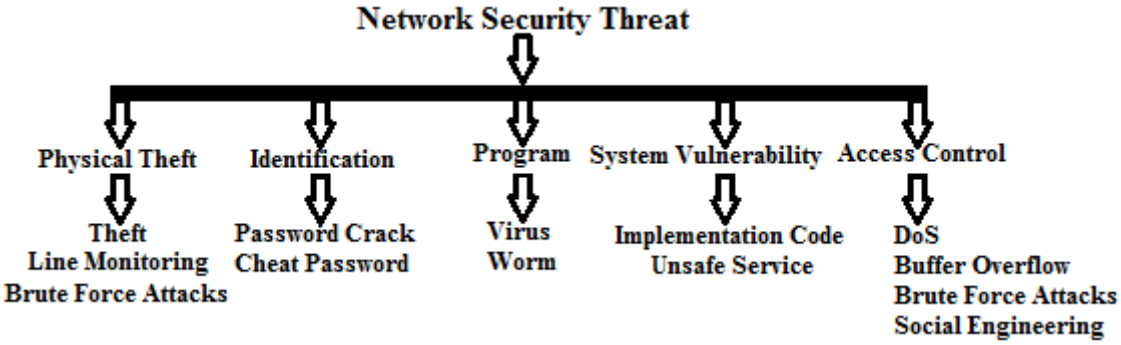

Fig.1. Classification of Network Security Threats

II. PROBLEMS IN CAMPUS NETWROKS

The problem related to campus networks are the type of media to be used between buildings, outside cable specifications, rights-of-way, avoidance of natural barriers, underground or aerial cabling requirements, line of site for inter-building wireless transmissions, and security problem. Figure 1 shows classification of security threats. In campus network if cable is open than it can be tapped or cut. A user within the company can access many internal resources. There may be no any bypass firewalls or other security mechanisms which prevent non-trusted sources, such as Internet users, to access the internal network. Such type of internal users can be equipped with hacking skills, and they can successfully penetrate and achieve remote administrative network rights. In fact number of network attacks originates from inside the firewall. Poor network security means that an external hacker break into a computer. on network, then they can access the rest of the internal network more easily. This would enable the attacker to read and possibly leak confidential emails and documents; trash computers, leading to loss of information; and more. The University network must be kept secure. Security concerns involve protection of central data files, host computers and the network itself. Tracking of virus infections, compromised computers, and collaborating with other sites to isolate problems is an ongoing task. The technique most often used when problems occur is to quarantine the problem computer from the remainder of the University network by disabling its network port. This happens daily and sometimes many times each day during virus outbreaks. Clearly, a single-port model minimizes the interruption of services in a security incident. With network authentication, it will be possible to contact the person responsible for the computer to announce that the device has been quarantined, thereby saving time and confusion for the user. The campus network faces a serious security situation. The campus network has been a congregation of hackers. This is because the virus and hacker tools are spreading and most users are unconscious about security. In addition, college students are energetic and curious about new things. They have high intelligence and passion, but lack of the responsibility for the results of their behaviour. Malicious attacks of campus network are from the internal network. Wireless link makes the network more vulnerable from passive eavesdropping to active interference have variety of attacks. Since wireless networks transmit data through the electromagnetic waves in the air, within the transmitter coverage area all of the wireless.

Network users in campus can access to these data, as long as the frequency with the same receiver may get the message. In Campus WLAN, the threat that can be encountered mainly in the following areas: information disclosure, integrity destruction, denial of service and the illegal use of it. In general, network traffic is non-encrypted format, the attackers can easily monitor and crack wireless network communication packets. Intruders do not need to trap the eavesdrop or analytical equipment physically access the network, so the threat has become one of the biggest problems of wireless local area network.

III. PROPOSED SOLUTIONS FOR CAMPUS NETWORK INFORMATION SECURITY PROBLEM

To build more security robust campus network, we should analyze security risk, and on the basis of that, prepare unified plan to take action. We should adopt more and more advanced technology generously in our network e.g. Firewall technology, virtual Local Area Network (VLAN), encryption technology, Virtual Private Network (VPN), multiple operating system at server side etc.

In campus network we can use virtual private network (VPN) technology which uses special software on each computer (i.e. VPN client), to encrypt network traffic from that computer to a VPN concentrator on the institution's network. Generally, we do not use VPN on-campus, as the functionality that VPN provides is already present on campus. However, it would be more theft and misuse proof on Wireless Network. It can also be used to authenticate via VPN. Through VPN, member of campus computer can connect securely.

WLAN (Wireless Local Area Network) technology played an important role in promoting the development of campus information technology, and it is an important component in campus network. WLAN reduce the workload of the network cabling. Once it is completed, it becomes very easy to the users to access the network at any location in the campus. PKI technology, and achieve centralized configuration, monitoring, management. Finally, we should strengthen formulating of systems and specifications about the network security.

Any user, user group, or department wants to establish its own local area network or to establish connectivity to external data communications networks must assign a member of that user group or department to coordinate with Network Services and obtain approval. Colleges and Administrative units may create sub domains within campus network. Sub domains usually encompass multiple departments which have a need to share common information. System should automatically alert the security event to the user, if security problem is detected as well as user should be isolated to the recovery area or block the data

flows according to the user ID Computer viruses and worms are the most common security problems in campus network, and these viruses are written for any operating system to exploit security flows. Different viruses are written for different operating system that can run on particular type of operating system (For example Linux-Unix, Microsoft Window, MAC OS etc.). Therefore two types of operating systems (having different kernel architecture) should be used in server center in pipeline, allowing all traffic to go through this pipeline and activity analysis should be done on both systems separately. Unused port should always be closed on server. Improper use of the security settings will also increase the security vulnerabilities. In addition the operating system's security problems generate from the virus threats. Hackers penetrated the network to destruct the data. Network antivirus tools must be effective and kept updated to protect all possible virus entry from the internet. Anti-virus program should be installed for online virus detection and the virus clean-up or tracking. Intrusion detection sensors should be placed at the campus border to identify computers, generating infected and malicious traffic entering or leaving the campus computing network. A network honeypot should also be placed on an unused network segment to identify infected computers attempting to scan or connect to nonexistent hosts. Figure 2 shows a standard layout diagram for campus network establishment

The network security must be all-around the campus. More network security measures must be in the important areas such as network outlet, data center, and servers. After that both the access or backbone equipment must be equipped with strong defense ability, and the deployment of security policies must not affect the network performance or cause single point failure. Overall the security must be deployed globally to cover every aspect, from access control, detailed detection of security events, and collaboration of existing security equipment, to accurate location of threat source and isolation and recovering according to user ID, further the entire security structure of the network is formed from internal to external network.

Therefore, in the security deployment some key areas like outlet, security measures shall be extended to the whole network to make a big move beyond the equipment level security, rather than enforce the security strength of single local points.

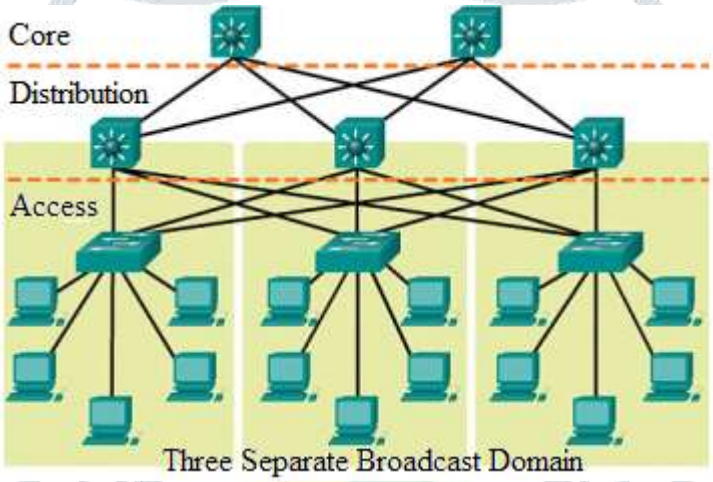

Fig. 2. Standard layout graph for campus network establishment

IV. CONCLUSION AND FUTURE WORK

In short, by providing network security in campus, the teachers and students can teach, work, study, research at anytime, anywhere in campus. A secure network plays a vital role for promoting the development of campus information and digital campus construction. This paper proposed a viewpoint from access control, data sharing management, content filtering, data encryption, user management, permissions distribution, log auditing, and several other security issues. As network security has become more and more important, the proper protection have to be built to achieve the open and secure network environment we aimed for.

REFERENCES

[1] S. Saadat M. Network Security Principles and Practices (CCIE Professional Development) (CCIE Professional Development) (Hardcover) [M].Cisco Press, 2007: 52-78.

[2] William S. Network Security Essentials: Applications and Standards (3rd Edition) (Paperback) [M]. Oxford:Blackwell business, 2006: 15 – 47.

[3] Mark R, Roberta B, Keith S. Network Security: The Complete Reference [M]. Osborne: McGraw-Hill Osborne Media, 2003-11-17.

[4] Kwot T.Fung Network Security Technologies, Second Edition [M]. AUERBACH,2004/10/28, 11-123.

[5] Joel S, Stuart M, George K. Hacking Exposed: Network Security Secrets & Solutions [M]. McGraw-Hill, April 2005:23-126.

[6] B. Harris, R. Hunt. TCP 1 IP security threats and attackmethods .Computer Communications, 1999, (22) :Page.885-897

[7] Venter H S, Eloff J H P. Data packet intercepting on the internet: how and why? A closer look at existing data packet - intercepting tools .Computers & Security, 1998, 17(3):683-692

[8] SHEN ChangXiang, ZHANG HuangGuo et al. Survey of information security. SHEN ChangXiang et al. Sci China Ser F - Inf Sci I June 2007 I vol. 50 I no. 3 I 273-298

[9] Yong Yu, Wireless Distribution System Management , WHUT,2007.5